Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	CG Docket No. 96-115 RM-11277

COMMENTS OF CHARTER COMMUNICATIONS, INC.

Christin McMeley
Vice President & Senior Counsel
Privacy & Regulatory
Charter Communications, Inc.
12405 Powerscourt Drive
St. Louis, MO 63131

John D. Seiver
Timothy P. Tobin
Brian J. Hurh
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
(202) 659-9750

Attorneys for Charter Communications, Inc.

April 28, 2006

SUMMARY

Charter acknowledges that the theft of CPNI is an important issue to consumers. However, the Commission's implementation of new requirements for service providers as proposed by the Electronic Privacy Information Center (EPIC) would ignore the source of the problem – pretexters who fraudulently obtain CPNI – and instead would impose counterproductive mandates on service providers that would only raise costs for providers and in turn consumers, make it harder for service providers to adapt to new tactics and threats from pretexters, and slow the deployment of competitive alternatives to traditional telecommunications carriers. Regardless of what mandates the Commission embraces, bad actors will continue to devote substantial efforts toward defeating security measures. Therefore, it is important for the Commission to recognize that existing rules already provide significant protections for CPNI especially when combined with the extensive competitive and public perception incentives that providers have to protect CPNI. These market incentives have increased dramatically in the last few months with the publicity surrounding pretexting. As a result, providers have, and will continue, to review and update their practices to enhance the protection of CPNI.

Accordingly, the best way to protect CPNI is through the vigorous pursuit of pretexters and other wrongdoers. Over the last few months, federal and state law enforcement entities and telecommunications carriers have all instituted legal actions against pretexters and this is already dramatically slowing the incidents of pretexting. The best way for the Commission to assist in the pursuit of prextexters is by coordinating with the Federal Trade Commission and State Attorneys General and enforcing existing rules where necessary.

If the Commission decides it must adopt new rules, rather than impose rigid new technological mandates and practices, the Commission should require carriers to implement

"reasonable" safeguards. Under such an approach, carriers would vigilantly monitor threats and reformulate practices in response to any new threats. It would also allow the Commission to consider how carriers have tailored CPNI protections to their individual characteristics, culture and technological capabilities since what might work for one organization might not for another. If the Commission does enact specific technological mandates and practices, it should implement a safe harbor that providers could comply with to avoid being liable for violations of the rules when they have acted in good faith.

The Commission should also not extend CPNI rules to VoIP providers at this time. The Commission should resolve the regulatory classification of VoIP as either a telecommunications or information service prior to considering extension of CPNI rules to that service. If the Commission were to classify VoIP as an information service, the Commission would be without jurisdiction under current law to apply its rules to VoIP providers.

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	CG Docket No. 96-115 RM-11277

COMMENTS OF CHARTER COMMUNICATIONS, INC.

I. INTRODUCTION

Charter Communications, Inc. and its affiliates ("Charter" or the "Company") acknowledge the great concern resulting from the widely publicized theft of CPNI. Nonetheless, the Commission should not lose sight of to whom these "disclosures" were made: pretexters who fraudulently tricked carriers' customer service representatives into revealing this closely held information. While the Commission, Congress and the public are all reasonably concerned about whether carriers have adequate procedures in place to protect CPNI, decision-makers should bear in mind that carriers are also the victims of these illegal pretexting schemes. Nothing can make customers switch service providers faster than news that pretexters or other bad actors obtained their confidential information.

Therefore, as the Commission considers changes to the CPNI rules, the Commission should bear in mind that carriers already have every incentive to protect their customers'

confidential information and comply with the current CPNI rules, which when combined with adequate enforcement and pursuit of thieves, provides significant consumer protection. The current rules contain a number of safeguards and substantial restrictions on how CPNI can be used and shared. The Notice of Proposed Rulemaking ("NPRM") to which these Comments are directed,[1] however, indicates that the Commission is considering new rules that could impose very specific procedural requirements on carriers' operations, in addition to new requirements on how CPNI must be handled and steps carriers must take if there is even a suspicion of disclosure.

Charter believes that these proposed requirements are a mistake. No system is fool-proof and it would be counter-productive for the Commission to try to mandate specific requirements into carriers' operations. There are already sufficient competitive and public perception incentives for carriers to protect CPNI without the need for burdensome new regulatory mandates for telecommunications carriers. Additional rules will interfere with carriers' operations, actually making it more difficult to respond to new technological threats. They will also add costs on companies, and ultimately customers, without a proportionate benefit to those customers. New rules will particularly burden new entrants like Charter, who are among the few entities that can provide meaningful facilities-based competition with traditional telecommunications carriers.[2] The added costs and administrative complexity could slow deployment of VoIP and VoIP based services.

---

[1] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, Notice of Proposed Rulemaking, CC Docket No. 96-115 (Feb. 14, 2006) (hereinafter *CPNI NPRM*).

[2] *See, e.g., In the Matter of Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers*, Report and Order and Order on Remand and Further Notice of Proposed Rulemaking, 18 F.C.C.R. 16978, ¶ 32, at 17,006 (Aug. 21, 2003) ("[T]he goals of the 1996 Act . . . include[e] the rapid introduction of competition, ***promotion of facilities-based***

The appropriate focus should instead be on punishing wrongdoers – those that surreptitiously obtain CPNI from carriers for personal gain. Vigorous enforcement is the most effective deterrent. Regardless of what mandates the Commission embraces, bad actors will continue to devote substantial efforts towards defeating whatever security measures that the industry implements. Accordingly, Charter urges the Commission to enhance its existing rules by stepping up enforcement where necessary, and in conjunction with the Federal Trade Commission ("FTC") and State Attorneys General, by pursuing thieves – the real threat to consumers – who attempt to steal CPNI.

If the Commission nonetheless decides to amend its CPNI rules, it should not dictate specific sweeping security mandates and practices. Instead, it should allow carriers to implement "reasonable" measures appropriate to their specific operations and business needs.

Part II of these Comments provides background information on Charter. Part III then explains that enforcement of existing rules coupled with market incentives and pursuit of pretexters will best protect consumers. Part IV addresses in detail why the current opt-in/opt-out regime is sensible. Part V explains why the Commission's proposed safeguards are unnecessary and why a "reasonableness" standard is preferable. Part VI discusses the Commission's lack of jurisdiction to extend CPNI rules to VoIP-based services and lastly, Part VII states that if the Commission does amend its rules, it should adopt a safe harbor.

II. ABOUT CHARTER

Charter is a broadband communications company with over 6 million customers in 38 states. Through its broadband networks, Charter offers a full range of advanced broadband

---

competition, investment and innovation, certainty in the market place, ***administrative practicality and reduced regulation.***") (emphasis added); *id.* ¶ 354 n.1069, at 17,195 (refers to "the encouragement of facilities-based competition" as "one of our ***principal objectives*** in implementing the Act) (emphasis added).

services, including traditional cable video programming (both analog and digital), high-speed cable Internet access, advanced broadband cable services (such as video on demand ("VOD"), high definition television service ("HDTV") and interactive television) and voice service, primarily through Voice over Internet Protocol ("VoIP") technology over its cable networks. Charter current serves over 190,000 voice communications subscribers, the vast majority of which are served with VoIP technology, and is continuing to aggressively roll out its VoIP based voice service. Making its voice services utilizing VoIP ("VoIP based voice service") available to customers throughout its service area is one of Charter's highest business priorities.

Therefore, when providing VoIP based service Charter is not a traditional "telecommunications carrier."[3] Nonetheless, prior to even offering VoIP based voice service, as a natural outgrowth of the privacy protections required by the Cable Act[4] – which applies to all services offered by Charter – Charter put procedures in place to protect its customers' personally identifiable information ("PII"). The Cable Act requirements include customer opt-in and opt-out approval mechanisms depending on the type of PII, customer access to PII, record destruction requirements, customer notice of rights, and a requirement "to take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[5] Therefore, like Section 222, the Cable Act does not mandate specific practices or technological standards. Most of Cable Act PII requirements have been in place since 1984, resulting in a longstanding culture of respect for customer privacy rights within

---

[3] 47 U.S.C. § 153(44).

[4] 47 U.S.C. § 551; *see also* Center for Democracy and Technology, Guide to Online Privacy, Chapter Three: Existing Federal Privacy Laws, http://www.cdt.org/privacy/guide/protect/laws.shtml ("The Cable Act establishes a comprehensive framework for cable regulation and sets forth strong protections for subscriber privacy . . . ." (citing Cable Communications Policy Act of 1984)).

[5] 47 U.S.C. § 551(c)(1).

the cable industry and at Charter. Cable operators such as Charter have a history of diligently protecting consumer records without the need for specific technological mandates imposed by Congress or regulators.

Although Charter recognizes that there is a lack of clarity regarding whether Section 222 and the Commission's CPNI regulations directly apply to Charter's VoIP based voice service, Charter determined when it first rolled-out VoIP based voice service in Wausau, Wisconsin in 2002, that compliance with the CPNI rules makes good business sense by honoring its customers' privacy interests and expectations. Accordingly, Charter expanded its PII procedures to include the additional CPNI protections to its VoIP based voice service and has added additional safeguards to assure that its VoIP based voice service customers receive the same CPNI protections as customers of traditional telecommunications carriers.

III. THE COMMISSION SHOULD FOCUS ON ENFORCING THE EXISTING CPNI RULES AND ON HELPING TO PROSECUTE WRONGDOERS.

The Commission issued this NPRM in response to a petition by the Electronic Privacy Information Center ("EPIC") that expressed concerns about carriers' protection of CPNI.[6] The *EPIC Petition* discussed the availability of CPNI for sale on various websites and the boasts of "data brokers" who advertised their ability to obtain specific CPNI within relatively quick time frames.[7] According to EPIC, the "prevalence of this current practice and the possibility of further exploitation of lenient security standards create a significant privacy and security risk to carrier customers, one that must be addressed by prompt action by the FCC."[8] Charter agrees

---

[6] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, (Aug. 30, 2005) (hereinafter *EPIC Petition*).

[7] *CPNI NPRM* ¶ 1.

[8] *EPIC Petition* at 2.

with EPIC that the availability of CPNI and data brokers' advertised ability to obtain CPNI is a serious privacy concern. However, enacting new rules applicable to carriers will not resolve the problem. The fact is that no amount of regulation or technological requirements will provide absolute protection for CPNI. Enforcement of current rules and pursuit of pretexters, coupled with market forces, particularly in today's competitive environment, will dictate that carriers institute adequate levels of protection.

A. Existing CPNI Rules are Sufficient.

Under Section 222 of the Communications Act, Congress expressly imposed a duty on telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to ... customers."[9] Accordingly, the Commission's rules implementing Section 222 require telecommunications carriers to implement strong data protection safeguards, including establishing a system to track customer approval for use of CPNI,[10] training personnel and instituting a disciplinary process,[11] maintaining records of carriers' and affiliates' use of CPNI for marketing campaigns and disclosures to third parties,[12] requiring supervisory review of outbound marketing campaigns,[13] requiring an officer to sign an annual compliance certificate,[14] and mandating oversight of independent contractor or joint venture partners.[15] Moreover, the rules describe in detail the procedures carriers must follow to obtain opt-in or opt-out approval

---

[9] 47 U.S.C. § 222(a).

[10] 47 C.F.R. § 64.2009(a).

[11] *Id.* § 64.2009(b).

[12] *Id.* § 64.2009(c).

[13] *Id.* § 64.2009(d).

[14] *Id.* § 64.2009(e).

[15] *Id.* § 64.2007(b)(2).

from a customer to use or disclose CPNI for marketing purposes,[16] as well as detailed rules regarding customer notices.[17] Finally, the current rules specifically outline when a telecommunications carrier may use and disclose CPNI without customer approval.[18] These rules provide the basis for very meaningful customer control over how CPNI is used and requires carriers to implement practices and protocols to protect CPNI.

Charter's CPNI protection program is fully compliant with the Commission's current rules.[19] Charter opposes the addition of new and burdensome regulatory and technological mandates, which could slow Charter's attempt to roll-out competitive voice services by deterring further investment or by distracting investment from launching markets to implementing burdensome and unnecessary rules. The Commission itself recognized in its *Second Report and Order* that additional requirements may "dampen competition by increasing the costs of entry into telecommunications markets."[20] That remains true today.

B. The Marketplace Polices Businesses' CPNI Practices.

Protecting customers' CPNI and achieving marketplace success go hand in hand. As the Commission has previously noted, "the carrier with whom the customer has the existing business relationship has a strong incentive not to misuse its customers' CPNI or it will risk losing its

---

[16] *See generally* 47 C.F.R. §§ 64.2005 and 64.2007

[17] *See generally id.* § 64.2008.

[18] *See generally id.* § 64.2005.

[19] Charter respectfully declines to identify its specific practices to protect CPNI. Charter considers much of that information proprietary and, as the Commission has recognized, there is danger in "giving wrongdoers a roadmap." *CPNI NPRM* ¶ 25 (internal quotations omitted).

[20] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 F.C.C.R. 8061, 8197, ¶ 197 (Feb. 26, 1998) (hereinafter *Second Report and Order*).

customers' business."[21] As Charter and other VoIP based voice service providers expand their offerings, voice and video competition will continue to intensify.[22] Unlike the time when the Baby Bells and AT&T were the only, or almost only, telephone service providers with few, if any, viable alternatives, a consumer can now choose between the ILEC, the cable operator, other competitive LECs, non-facilities based VoIP providers, and wireless carriers.[23] In such an environment, incentives to serve customers by protecting their CPNI are particularly strong.

And nothing can alienate a customer like the improper handling of confidential information. For example, recent studies demonstrate that nearly 20 percent of customers immediately terminate service with companies that have lost their PII and an additional 40 percent of customers consider terminating their relationship with such companies.[24] In other words, nearly 60 percent of consumers either immediately terminate or consider switching or dropping a provider based on that company's failure to adequately protect PII.[25] In addition to

---

[21] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C.R. 14860, 14, 878, ¶ 37 (July 25, 2002) (hereinafter *Third Report and Order*); *see also id.* ¶ 37 n.109 ("[A]s competition continues to develop, this safeguard will only increase in its usefulness.").

[22] *See Availability of Advanced Telecommunications Capability in the United States*, Fourth Report to Congress, at 13, Sept. 9, 2004, http://www.cdt.org/privacy/guide/protect/laws.shtml ("[T]he competitive nature of the broadband market, including new entrants using new technologies, is driving broadband providers to offer increasingly faster service at the same or even lower retail prices.").

[23] *Id.* at 12 (finding that the increasing deployment of broadband is "critical for increasing popular uses of broadband, such as Voice over Internet Protocol (VoIP), interactive gaming, streaming media, and collaborative comuting, which are spurring demand today.").

[24] *Survey: Data Losses Spur Consumer Flight*, CIO TODAY, Jan. 27, 2006, http://www.cio-today.com/story.xhtml?story_id=123000030QXI (citing to survey conducted by Ponemon Institute Study and distributed by PGP Corp.).

[25] *Id.* Similar findings were made for customers of banks and other financial institutions. *See* Gene J. Koprowski, *Survey: Consumers Inclined to Switch Banks if Victimized*, ECOMMERCETIMES, Nov. 18, 2005, http://www.ecommercetimes.com/story/47422.html (reporting that a recent survey commissioned by Sun Microsystems indicates that 50 percent of

customer loss, the marketplace also punishes businesses by directly impacting share and brand value. For example, the Wall Street Journal has noted that companies suffering publicized security breaches in which confidential customer data was compromised experienced a reduction in stock prices.[26]

Accordingly, communications providers already have strong market incentives to protect CPNI, which have been enhanced by the widespread outrage and publicity surrounding the actions of those data brokers and private investigators who, in some instances, have been able to obtain CPNI. Providers, including Charter, have reassessed their practices in light of these incidents, not because of any new rules or regulations.

C. Enforcing Existing Laws Against Wrongdoers is the Proper Approach.

In addition to carriers modifying their practices in response to competitive and market pressures, the most effective way to safeguard CPNI is to enforce existing laws and punish those who engage in pretexting[27] and other illegal activities to obtain CPNI. Focusing on new regulatory requirements is unwarranted. Even EPIC, whose concerns prompted this NPRM, recognized that "telecommunications carriers are not responsible for actively disseminating information to unauthorized third parties. Rather, unauthorized third parties have been exploiting security standards at the carriers to access and sell the information acquired through

---

consumers would take their online business elsewhere if they were victims of identity theft at a particular financial institution).

[26] Michael Rapaport, *Companies Pay a Price for Security Breaches*, THE WALL STREET JOURNAL, June 15, 2005, at C3.

[27] Pretexting is the act of pretending to be someone else to get information. *See* Dave Gussow, *Verizon Lawsuit Says Phony Callers are Committing Fraud*, ST. PETERSBURG TIMES, Jan. 30, 2006, *available at* http://www.sptimes.com/2006/01/30/news_pf/Technology/Verizon_lawsuit_says_.shtml. *See also CPNI NPRM* at ¶ 11 and n. 34 (describing pretexting and explaining the practice is also referred to as ("social engineering").

illegal means."[28] In only the few months since "pretexting" became widely publicized, there has been an overwhelming reaction from telecommunications carriers, lawmakers, regulators and law enforcement to address wrongdoers' actions.

First, the Commission launched an investigation to determine how data brokers are obtaining CPNI.[29] Part of this investigation included the Commission's issuance of subpoenas to approximately 32 data brokers to determine how they were obtaining CPNI and the subsequent issuance of citations to two companies subject to the subpoenas because of their failure to respond.[30] Second, the FTC has vowed that it will pursue aggressive law enforcement actions against companies that steal CPNI through pretexting or other means under its authority to enforce unfair or deceptive trade practices pursuant to Section 5 of the Federal Trade Commission Act.[31] Third, federal and state lawmakers have introduced several bills to further

---

[28] *EPIC Petition* at 5.

[29] *See* Written Statement of Kris Ann Monteith, Chief, Enforcement Bureau, Federal Communications Commission, Before the Subcommittee on Consumer Affairs, Product Safety and Insurance, Committee on Commerce, Science and Transportation, U.S. Senate, *Protecting Consumers' Phone Records*, Feb. 8, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263731A1.pdf; *see also* Written Statement of Kevin J. Martin, Chairman, Federal Communications Commission, Before the Committee on Energy and Commerce, U.S. House of Representatives, *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?*, Feb. 1, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263577A1.pdf.

[30] *See* Official Citation to LocateCall.com, 1st Source Information Specialists, Inc., File No. EB-05-TC-059, Jan. 20, 2006 (citation for failure to comply with FCC order to produce documents and information), *available at* http://www.fcc.gov/eb/Orders/2006/DA-06-124A1.html; *and* Official Citation to DataFind.org, Data Find Solutions, Inc., File No. EB-05-TC-066, Jan. 20, 2006, *available at* http://www.fcc.gov/eb/Orders/2006/DA-06-122A1.html.

[31] 15 U.S.C. § 45; *see also* Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science and Transportation, Subcommittee on Consumer Affairs, Product Safety and Insurance, U.S. Senate, *Protecting Consumers' Phone Records*, Feb. 8, 2006, *available at* http://www.ftc.gov/os/2006/02/commissiontestimonypretexting060208.pdf; Prepared Statement of the Federal Trade Commission Before the Committee on Energy and Commerce, U.S. House of Representatives, *Phone Records for Sale: Why Aren't Phone Records*

address the problem of pretexting.[32] Although pretexting is already illegal under various state and federal consumer protection laws,[33] most of these new bills would explicitly make the practice of pretexting illegal with enhanced penalties. It is notable that the vast majority of these legislative proposals do not impose extensive new requirements on carriers, but rather focus on those who obtain CPNI under false pretenses or who sell CPNI that was initially obtained under false pretenses.[34] Fourth, state Attorney Generals in several states, including Texas,[35] Florida,[36]

Safe From Pretexting?, Feb. 1, 2006, *available at* http://www.ftc.gov/os/2006/02/commissiontestimonypretexting.pdf.

[32] Congress has introduced, just since the beginning of this year, at least 10 bills to address the pretexting problem: H.R. 4657, H.R. 4662, H.R. 4678, H.R. 4709, H.R. 4714, H.R. 4993, S. 2177, S. 2178, S. 2264, and S. 2389. State lawmakers in at least 16 states, including Alabama, Arizona, California, Connecticut, Colorado, Florida, Georgia, Illinois, Maine, Maryland, Minnesota, Missouri, Oklahoma, Virginia, South Dakota, and Washington, have introduced their own legislation to expressly make pretexting illegal.

[33] State Attorneys General have generally resorted to their states' respective consumer fraud and deceptive business practices laws to go after data brokers. *See, e.g.*, News Release, Attorney Abbott Files First Suit Against Sellers of Private Phone Records (Feb. 9, 2006) (Texas lawsuit filed pursuant to Texas Deceptive Trade Practices Act), http://www.oag.state.tx.us/oagnews/release.php?id=1449; News Release, Crist: Websites Hawking Phone Records Shut Down (Feb. 9, 2006) (Florida lawsuit pursuant to Florida's Unfair and Deceptive Trade Practices Act), *available at* http://myfloridalegal.com/newsrel.nsf/newsreleases/40265981391EDECE8525711000659BA9; Press Release, Madigan Sues Company That Buys Cell Phone Records (Jan. 20, 2006) (Illinois lawsuit filed under Illinois Consumer Fraud and Deceptive Business Practices Act), *available at* http://www.ag.state.il.us/pressroom/2006_01/20060120.html. Regarding federal law, *see supra*, note 32.

[34] Of the 10 federal bills listed in *supra*, note 32, only one, H.R. 4943, would significantly revise the Commission's current FCC rules applicable to carriers through extensive amendments to Section 222. Two others, H.R. 4993 and S. 2389 would also direct the Commission to initiate a rulemaking to establish safeguards as would S. 2389. Notably, under S. 2389, these safeguards must be similar to the FTC's GLBA Safeguards Rule applicable to financial institutions, which does not mandate specific safeguards but rather requires security programs that are appropriate to the size, complexity and nature of each business. *See infra*, Section V.A. (discussing the FTC's GLBA safeguard rules); *see also* 16 C.F.R. § 314.1—314.5. A fourth bill, S. 2264, would codify existing FCC rules under Section 222 with some minor variations. Most aspects of the seven other bills, including the only bill to pass in one of the two full chambers of Congress, H.R. 4709, either focus exclusively or primarily on the actions of pretexters and others who surreptitiously try to obtain CPNI. Of the various pending state proposals, only a few bills focus on telecommunications carriers. *See, e.g.*, Georgia S.B. 456 and Connecticut H.B. 5783.

Illinois,[37] and Missouri[38] have brought enforcement actions against pretexters. Finally, telecommunications carriers themselves have filed lawsuits against data brokers that obtained their customers' CPNI.[39]

The overwhelming response by state and federal law enforcement, regulators, lawmakers and telecommunications carriers is making an impact and proving to be an effective deterrent.[40] As a result of these actions, over twenty web sites that previously offered CPNI for sale have

---

[35] *See State of Texas v. USASkipTrace.com*, Plaintiff's Original Petition and Application for Temporary Restraining Order, Cause No. ___ (Dist. Ct. Travis County Tex., Feb. 9, 2006), *available at* http://www.oag.state.tx.us/newspubs/releases/2006/020906skiptrace_pop.pdf.

[36] *See State of Florida v. 1st Source Information Specialists, Inc.*, Complaint for Injunctive and Other Statutory Relief, Case No. __ (Cir. Ct. Leon County Fla., Jan. 24, 2006), *available at* http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6L8KGC/$file/1stSource_Complaint.pdf.

[37] *See* Press Release, Madigan Sues Company That Buys Cell Phone Records (Jan. 20, 2006) (reporting lawsuit filed against 1st Source Information Specialists, *et. al.* in Sangamon County Circuit Court), *available at* http://www.ag.state.il.us/pressroom/ 2006_01/20060120.html.

[38] *See State of Missouri v. Data Find Solutions Inc., et. al.*, Case No. 06AC-CC00067 (19th Judicial Cir. Ct. Mo., Jan. 20, 2006); *see also State of Missouri v. Data Trace USA Inc, et. al.*, Case No. 06AC-CC00158 (19th Judicial Cir. Ct. Mo., Feb. 6, 2006).

[39] Telecommunications carriers have filed their lawsuits in both state and federal court. *See, e.g., Cingular Wireless LLC v. Data Find Solutions Inc., et. al.*, Civil Action File No. 1:05-cv-03269-CC (N.D. Ga. filed Dec. 23, 2005); *Cellco Partnership d/b/a/ Verizon Wireless v. Data Find Solutions et. al.*, Civil Action No. 3:06-cv-00326-SRC-JJH (D.N.J. filed Jan. 24, 2006); *Cingular Wireless LLC v. Global Information Group Inc. et. al.*, Civil Action File No. 1:06-cv-00413-TWT (N.D. Ga. filed Feb. 23, 2006); *Spring Nextel Corp. v. San Marco & Assocs., et. al.*, Civil Action File No. 8:06-cv-00484-EAK-TGW (M.D. Fla. filed March 17, 2006); *T-Mobile USA Inc. v. First Source Information Specialists Inc., et. al.*, Case No. 06-2-03113-0 (King County Sup. Ct. filed Jan. 23, 2006); *Sprint Nextel Corp. v. All Star Investigations Inc.*, Local Case No. 2006-1736-CA-01 (Miami-Dade County Ct. filed Jan. 27, 2006); *Sprint Nextel Corp. v. First Source Information Specialists*, Case No. CACE06001083 (Broward County Fla. filed Jan. 26, 2006).

[40] *See, e.g., Missouri First State to Force Web Business to Stop Selling Cell Phone Records*, Missouri Attorney General's Office, January 30, 2006, *at* http://moago.org/newsrelease/2006/013006b.htm; *see also Locatecell.com Must Stop Selling Cell Phone Records of Missourians, Under Court Order Obtained by Nixon*, Missouri Attorney General's Office, February 15, 2006, *at* http://moago.org/newsreleases/2006/021506.htm.

shut down or stopped advertising.[41] It is evident that the appropriate focus of the Commission and law enforcement generally should be on the law breakers and on enforcement of the current rules.[42] There is simply no need to impose new requirements on carriers.

IV. THE EXISTING OPT-OUT/OPT-IN REGIME SERVES CONSUMER'S INTERESTS.

The Commission's current rules protect consumer confidentiality by empowering consumers with choice regarding how carriers handle their CPNI. Under the current rules, carriers can share CPNI with affiliated entities from whom the customer receives certain telecommunications service – i.e., local, long distance or wireless – without customer consent.[43] Carriers must obtain "opt-out" customer approval to share CPNI with affiliates, joint venture partners or independent contractors to market "communications-related services" that the customer does not already receive from these other entities.[44] To share CPNI with an affiliate to market non-communications-related services, i.e., any other service, including cable video

---

[41] *See Web Sites Hawking Phone Records Shut Down*, MSNBC.COM, Feb. 9, 2006, http://msnbc.msn.com/id/11256418.

[42] In cases where a particular carrier is not in compliance with current rules, appropriate enforcement action by the Commission will help to further protect CPNI. *See, e.g., In the Matter of AT&T Inc.*, Notice of Apparent Liability of Forfeiture, File No. EB-06-TC-059 (Jan. 30, 2006) (notice for failure to have corporate officer with personal knowledge execute an annual certificate pursuant to 47 C.F.R. § 2009(e)); *In the Matter of Alltel Corp.*, Notice of Apparent Liability of Forfeiture, File No. EB-06-TC-058 (Jan. 30, 2006) (same); *In the Matter of CBeyond Communications, LLC*, Notice of Apparent Liability of Forfeiture, File No. EB-06-IH-0840 (Apr. 21, 2006) (same).

[43] *See* 47 C.F.R. § 64.2005(a). CPNI can also be disclosed in the provision of certain enumerated information services (which does not include Internet access) without consent. *See* 47 C.F.R. § 64.2005(b)(1).

[44] 47 C.F.R. § 64.2007(b)(1). "Communications-related services" in the context of the CPNI rules include telecommunications services, Internet access service and certain other information services typically provided by telecommunications carriers, services related to customer premises equipment.

service, or to disclose CPNI to an unaffiliated third party, carriers must obtain opt-in consent from the customer.[45]

The Commission is seeking comment on whether it should require carriers to obtain a customer's express opt-in approval before disclosing CPNI to joint ventures and independent contractors that provide communications-related services.[46] The Commission also seeks comment on an alternative proposal to allow customers to place a total "no release" hold on all CPNI.[47] Both proposals are unnecessary and would burden businesses without an equivalent, corresponding benefit to consumers.

A. Opt-out for Joint Venture Partners and Independent Contractors Sufficiently Protects CPNI.

It is apparent to Charter that any change to the current regime for disclosing CPNI to joint ventures and independent contractors is unnecessary. Although Charter does not use CPNI to market its services now it may in the future and it often relies on independent contractors to market its services.[48] Consequently, reacquiring opt-in to share CPNI with independent contractors involved in marketing could severely impede Charter's ability to reach its

---

[45] 47 C.F.R. § 64.2007(b)(3).

[46] *CPNI NPRM* ¶ 12.

[47] *CPNI NPRM* ¶ 24.

[48] Charter also relies on third party carriers for underlying transport of traffic or for switching and connectivity of calls to other carriers. As a necessary part of this process carriers may exchange originating number identification and other information necessary send to send calls which can be matched to specific customers. Charter's understanding is that this type of information sharing is not prohibited by the CPNI rules. *See, e.g.*, 47 C.F.R. § 64.2007(b) (regarding approval processes for disclosing CPNI "for the purpose of marketing communications-related services); 47 U.S.C. § 222(d)(1). Without this sharing, it could not provide service to customers. To the extent any uncertainty exists over this type of information sharing, Charter requests the Commission provide clarification.

customers[49] and would disrupt the proper and fair balance between consumer and commercial interests that the current opt-out regime currently provides.

The Commission's current opt-out regime applicable to joint ventures and independent contractors implemented in its *Third Report and Order* reflects long-standing principles of promoting consumer protection while preserving commercial interests when it comes to regulating business practices. As Congress recognized when it enacted Section 222:

> The protections contained in section 222(b) and (c) represent a careful balance of competing, often conflicting, considerations. First, of course, is the need for customers to be sure that personal information that carriers may collect is not misused; this consideration argues for strict controls on a carrier's use of all customer data. Customers, on the other hand, rightfully expect that when they are dealing with their *carrier* concerning their telecommunications services, the *carrier's employees* will have available all relevant information about their service. This consideration argues for looser restrictions on internal use of customer information.[50]

With its *Third Report and Order*, the Commission achieved this balance with its opt-in/opt-out rules. In fact, the *Third Report and Order* was a deliberate and measured response to the Tenth Circuit's determination in *U.S. West v. FCC* that the Commission's earlier order

---

[49] *See See* Michael E. Staten & Fred H. Cate, *The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE. L.J. 745 (2003) ("[A]n opt-in system sets the default rule to 'no information flow,' under the presumption that consumers harbor greater concern about the risk of information usage than the loss of benefits consequent to shutting off the flow. Under an opt-in system, those benefits evaporate unless consumers explicitly grant permission for information about them to flow in the pipeline."). *Id.* at 766 ("By setting the default rule to 'no information flow,' an opt-in system restricts the information lifeblood on which today's economic activity depends.").

[50] H.R. REP. NO. 104-204, Pt. 1 at 90 (1995) (emphasis added). The balancing of consumer privacy interests and commercial interests is undertaken in virtually all privacy law regimes. For example, in implementing an existing business relationship exception to its Do-Not Call rules under the Telephone Consumer Protection Act, 47 U.S.C. § 227, the Commission acted consistent with Congress' express finding that "[i]ndividuals' privacy rights, public safety interests, and commercial freedom of speech and trade must be balanced in a way that protects the privacy of individuals and permits legitimate telemarketing practices," Similarly, the Commission, in developing its current opt-in/opt-out formula balanced similar considerations, and chose opt-out for those situations involving the marketing of communications related services by joint venture partners and independent contractors.

implementing a total opt-in regime, not unlike the Commission's current proposal, was unconstitutional.[51] In concluding that the opt-in approach violated the First Amendment, the court applied the traditional "narrow tailoring" standard applicable to commercial speech cases: the restriction "must be 'no more extensive than necessary to serve [the stated] interests,'"[52] and while "the government need not employ the least restrictive means to accomplish its goal, it must utilize a means that is 'narrowly tailored' to its desired objective."[53] The court further explained that a restriction need "not necessarily be perfect, but reasonable."[54] The Court found that the Commission, in implementing its initial rules under Section 222, failed to adequately consider customer opt-out consent, an "obvious and substantially less restrictive alternative."[55]

Following *U.S. West*, the Commission concluded in its *Third Report and Order* that "opt-out is an appropriate approval mechanism for the sharing of CPNI with, and use by, a carrier's joint venture partners and independent contractors in connection with communications-related services" because it "directly and materially advances the government's interest" in protecting CPNI "while also burdening no more carrier speech than necessary."[56] The Commission reached this conclusion by analogy to its opt-out choice for sharing CPNI with affiliates for marketing communications-related services, which the Commission is not proposing to change.[57] The

---

[51] *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert denied sub. nom. Comp. Policy Inst. v. U.S. West, Inc.*, 530 U.S. 1213 (2000).

[52] *Id.* at 1238 (citing *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 486 (1995)).

[53] *Id.* (citing *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993)).

[54] *Id.* (citing *Board of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989)).

[55] *Id.*

[56] *Third Report and Order*, 17 F.C.C.R. at 14, 875, ¶ 32.

[57] *See id.* at 14,880, ¶ 45 ("[T]he same factors we consider above [for affiliates offering communications-related services to which the customer does not subscribe] weigh in favor of allowing carriers to share CPNI based on opt-out approval with their agents, and with

Commission explained its affiliate-sharing approach as one based on customers' expectations and the benefits that accrue to them:

> [T]he record makes evident that a majority of customers nevertheless want to be advised of the services that their telecommunications providers offer. Furthermore the record establishes that customers are in a position to reap significant benefits in the form of more personalized service offerings (and possible cost savings) from their carriers and carriers' affiliates providing communications-related services based on the CPNI that the carriers collect. Enabling carriers to communicate with customers in this way is conducive to the free flow of information, which can result in more efficient and better-tailored marketing and has the potential to reduce junk mail and other forms of unwanted advertising. Thus, consumers may profit from having more and better information provided to them, or by being introduced to products or services that interest them. The empirical evidence indicating that a majority of customers want to be advised of service offerings from their carriers is consistent with the expectation that targeted carrier marketing will benefit them. Based on the th[e] record evidence, we think it is reasonable to conclude that targeted marketing of communications-related services using CPNI by the carrier that collects it is within the range of reasonable customer expectations. ... Thus, we conclude that an opt-out scheme giving customers an opportunity to disapprove intra-company uses of CPNI directly and materially advances customers' interest in avoiding unexpected and unwanted use and disclosure of CPNI and is sufficient to meet the 'approval' requirement under section 222.[58]

The Commission should not depart from its prior findings. In the *Third Report and Order*, the Commission alluded to joint venture partners and independent contractors, like affiliates, being from the customer's perspective, the same as the carrier itself.[59] The Commission noted in particular that "carrier burdens could be significant . . . under an opt-in scenario because opt-in could immediately impact the way carriers conduct business."[60]

---

independent contractors (such as telemarketers) and joint venture partners to market and provide communications-related services.").

[58] *Id.* at 14,876, ¶ 35.

[59] *See id.* ¶ 36 (referring to bundled services or products offered by affiliates) and at 14,881, ¶ 45 (finding the same factors applicable to affiliates apply to independent contractors and joint venture partners).

[60] *Id.* at 14,881, ¶ 45; *see also id.* at 14,881, ¶ 45 n.121 (noting that many carriers rely on independent contractors to perform telemarketing functions on their behalf). *See also* Steven

Particularly in today's era of convergence, Charter's affiliates (or independent contractors for other companies) may be indistinguishable from one another, particularly where a customer can receive a bundled "triple-play package" (voice, video and data) with consolidated billing. Customers simply view "Charter" as their provider or potential provider for all services, even though different affiliates (or in the case of other companies, independent contractors), might be the actual or potential provider.

The Commission also found that although opt-out makes it easier for carriers to obtain consent, it still provides customers with a meaningful privacy choice for their CPNI. In opt-out regimes, consumers that are truly concerned about their privacy can withhold their consent.[61] The Commission has designed the CPNI rules to provide an adequate opportunity for consumers to be informed of, and to exercise, their privacy choices at all times, by implementing numerous "choice safeguards" to preserve the customer's ultimate control over their CPNI. For example, under the current CPNI rules, carriers must give customers adequate notice and opportunity to opt-out every two years,[62] with the rules specifying in detail the content of such notification.[63] Charter not only mails customers CPNI notices every two years, it keeps its CPNI notice posted on its web site. In addition, after mailing notices, the carrier must then wait at least 30 days before assuming that the customer has consented, i.e., decided not to opt-out pursuant to the

---

Hetcher, Changing the Social Meaning of Privacy in Cyberspace, 15 HARV. J.L. & TECH. 149, 184 (2001) ("[S]imple corporate efficiency may require outsourcing various data-related activities necessary to a firm's own internal usage of the data.").

[61] *See* Staten, *The Impact of Opt-in Privacy Rules*, *supra* note 49, at 766 ("[O]pt-out presumes that consumers do want the benefits (greater convenience, wider range of services, and lower prices) facilitated by a free flow of information, and then allows people who are particularly concerned about privacy risks to remove their information from the pipeline.").

[62] 47 C.F.R. § 64.2008(d)(2).

[63] *Id.* at § 64.2008(c).

notice.[64] Even after a carrier has obtained the customer's opt-out approval, the carrier must additionally provide the opportunity to opt-out at no-cost to the customer, 24 hours a day, seven days a week.[65] Besides customer notice, the Commission also required that joint venture partners and independent contractors contractually adhere to CPNI protective measures.[66] Customer's ability to exercise choice and to stay informed of their options counsels against an opt-in approach for joint venture partners and independent contractors.

In addition to the opt-out privacy choice for customers, the Commission still requires opt-in for disclosures to other parties such as third parties and non-communications affiliates. The Commission noted a difference between those entities on the one hand, and affiliates, joint venture partners and independent contractors that provide communications-related services on the other. Disclosures of CPNI to the former entities would, according to the Commission, likely result in "far more substantial harms that are attendant upon unknowing and unwanted third-party disclosures"[67] Hence, requiring opt-in approval was more appropriate for disclosure to these entities.

Because consumers already have a relatively strong relationship with their carriers, carriers have an incentive not to misuse their existing customers' CPNI and risk losing their customers' business.[68] This relationship will only grow stronger as carriers increasingly provide

---

[64] *Id.* at § 64.2008(d)(1).

[65] *See Third Report and Order*, 17 F.C.C.R. at 14,912, ¶ 118 (allowing carriers the freedom to select the method for providing an opt-out mechanism, "so long as all customers are able to access and use those mechanisms, 24 hours a day, seven days a week."); *But cf.* 47 C.F.R. § 64.2008(d)(3)(v) (requiring a 24-hour, seven days a week, opt-out mechanisms under subsection for telecommunications carriers that use e-mail to provide opt-out notice).

[66] 47 C.F.R. § 64.2007(b)(2).

[67] *Third Report and Order*, 17 F.C.C.R. at 14,888, ¶ 62.

[68] *See discussion supra*, Part III.B.

bundled voice, video, data and other services. Requiring opt-in to share CPNI with affiliates, joint venture partners and independent contractors for marketing "communications related services" is not reasonable, given the greater connectivity between a carrier and the customer for communications-related services.

B. Total "No-Release" Hold Would Be Excessive.

The Commission also inquired whether it "[s]hould permit carriers to permit customers to put an absolute 'no release' order on their CPNI" possibly subject to certain statutory exceptions (such as for lawful law enforcement requests).[69] A total "no release" hold is excessive and unnecessary in light of the adequacy of the current opt-in/out-out regime. As explained above, the current regime allows carriers to use CPNI in a reasonable manner for the benefit of the subscriber, while protecting customers from the greater risk of CPNI misuse by non-communications affiliates and third parties.

Under the current regime, the only CPNI sharing a customer cannot prohibit through opt-in or opt-out is intra-affiliate sharing among affiliates that provide a service offering (local, long-distance, or wireless service) to the customer, i.e., the "total service approach." It would make no sense, and would actually infringe upon customer expectations, to expand a no-hold option to apply even to such affiliate sharing. The "total service approach" for using and sharing CPNI without customer consent coupled with the opt-in and opt-out consent for other choices reflects a reasonable accommodation of the varying interests.

The Commission adopted the "total service approach" in recognition of consumer expectations and marketplace realities. Specifically, it explained that "*[c]ustomers do not expect that carriers will need their approval to use CPNI for offerings within the existing total service*

---

[69] *CPNI NPRM* ¶ 24.

to which they subscribe."[70] The Commission found that in such instances, the customer "can be presumed to have given implied consent" for its carrier to use the CPNI for aspects of the services to which it subscribes from the carrier.[71] Moreover, as the Commission explained, the customer will view its service as the total service received from the carrier, including those from affiliates and subsidiaries:

> [C]ustomers would expect or desire their carrier to maintain internal divisions among the different components of their service, particularly where such CPNI use could improve the carrier's provision of the customer's existing service. ... [C]ustomers choosing an integrated product will expect their provider to have and use information regarding all parts of the service provided by that company, and will be confused and annoyed if that carrier does not and cannot provide complete customer service.[72]

The Commission's reasoning still rings true today. Accordingly, a total "no release" hold would not only interfere with customers' expectations and the long-established "total service approach," it would complicate internal processing of CPNI and increase overall costs,[73] especially when a customer subscribes to multiple services from the same carrier.

V. THE FCC'S PROPOSED SAFEGUARDS ARE UNNECESSARY AND TAKE THE WRONG APPROACH.

In its *CPNI NPRM,* the Commission proposes a series of new safeguards, which include but are not limited to, mandates for consumer-set passwords, encryption of stored CPNI, data retention limitations, including stripping or separating PII from other CPNI, notice requirements,

---

[70] *Second Report and Order*, 13 F.C.C.R. at 8,102-03, ¶ 55; *see also Third Report and Order*, 17 F.C.C.R. at 14,893, ¶ 76 ("we reaffirm our total service approach").

[71] *Second Report and Order*, 13 F.C.C.R. at 8,102-03, ¶ 55.

[72] *Id.*

[73] *See* Staten, *The Impact of Opt-in Privacy Rules*, *supra* note 49, at 766 (finding that under opt-in, "[c]ompanies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must restore the information flow by contacting one customer at a time to gain their individual permission to use information. Consequently, an opt-in system for giving consumers choice over information usage is always more expensive than an opt-out system.").

and a new audit trail requirement. Charter believes strongly that adopting these measures would be a mistake. Section 222 already imposes an affirmative duty to protect CPNI.[74] Protective measures that work for one company may not work for another. The Commission should, instead, focus its attention on the wrongdoers who steal confidential data and step-up enforcement of its current rules. Such an approach would provide adequate protection to consumers, but without imposing prohibitive and unanticipated costs on companies.

A. If the Commission Decides it Must Adopt New Rules, it Should Adopt a Case-By-Case Reasonableness Standard.

In 1999, the Commission reconsidered its Second Report and Order and lessened some of its CPNI regulation. It wanted to give "carriers the flexibility to adapt their record keeping systems in a manner most conducive to their individual size, capital resources, culture and technological capabilities."[75] The rationale for alleviating certain regulations in the *1999 Reconsideration Order* – allowing companies to adopt means to protect CPNI consistent with their unique circumstances, Section 222 and other Commission rules – applies equally today in favor of not imposing new additional mandates and requirements. Specifically, there is a risk that mandatory rules could "lock-in" certain security approaches and not be responsive to the evolving tools utilized by wrongdoers to access CPNI. Also, as explained in Part III above, Commission enforcement of its current rules, coupled with greater law enforcement against wrongdoers who seek to obtain CPNI, is the most sensible approach, and in fact is already having an impact. Although there have been well-publicized episodes of wrongdoers obtaining

---

[74] *See* 47 U.S.C. § 222 ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers . . . .").

[75] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 F.C.C.R. 14409, ¶ 7(f) (Aug. 16, 1999) (hereinafter *Reconsideration Order*).

and misusing CPNI in recent months, detailed technological mandates will likely result in regulatory overkill and are inconsistent with other approaches that are proving to be effective.

If the Commission decides it must enact new rules, the Federal Trade Commission's ("FTC") approach to obligations it places on companies to protect PII is particularly instructive. The FTC has established a flexible Safeguards Rule applicable to financial institutions under its authority under the Gramm Leach Bliley Act ("GLBA").[76] However, even outside of GLBA, the FTC has very broad authority under the Federal Trade Commission Act to prohibit "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce" applicable to businesses generally.[77] The FTC has recently begun using its "unfair practices" authority against non-financial companies' for failures to implement "reasonable" security procedures to protect consumers' PII and is imposing GLBA Safeguards Rule - type obligations on non-financial companies. It is becoming the *de facto* standard across industries.[78]

The FTC's approach in unfair trade practice cases is similar to the Commission's approach in the *1999 Reconsideration Order*. The FTC Chairman has said:

---

[76] 16 C.F.R. § 314.1-314.5.

[77] 42 U.S.C. § 45(a)(2). Although the FTC's authority under the Federal Trade Commission Act does not extend to telecommunications common carriers and certain other businesses, its jurisdiction is nonetheless quite broad and encompasses data brokers.

[78] *See, e.g., In the Matter of BJ's Wholesale Club, Inc.*, Decision and Order, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of DSW, Inc.*, Decision and Order, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, Agreement Containing Consent Order, FTC File No. 0523148 (Oct. 28, 2005). While the FTC has traditionally exercised its Section 5 authority only to pursue actions against entities that engage in deceptive acts, i.e., claiming they were protecting PII in a certain way while in practice not doing so, the FTC, as evidenced by these case has recently begun enforcing as "unfair practices", companies' failures to implement "reasonable" security procedures to protect consumers' PII, even when companies have not made specific privacy or security promises to customers.

> The laws and rules we enforce do not require that information security be perfect. That would be a costly, unobtainable standard. Rather, we require that a company's data security be reasonable in light of the nature of its business and the sensitivity of the information it handles.[79]

Reasonableness is inherently a fact-based inquiry taking into account the individual characteristics of each company. As part of consent decrees that the FTC has entered into under its unfair trade practices enforcement cases, the FTC has not mandated specific practices, but instead has imposed GLBA Safeguards Rule-type obligations on companies.[80]

The FTC's "reasonable" safeguards approach with vigilant business monitoring of threats and reformulation of practices in response to new threats is a sensible approach. It is one that the Commission should pursue if it believes that new rules are necessary. Because reasonableness is measured by current norms and practices, the Commission can more rapidly adjust its policies to respond to changes in the industry and react to evolving threats. Such an approach is more responsive than imposing specific mandates, especially in a situation like that with CPNI, where it is inherently difficult for an agency to mandate specific practices without the danger that those practices will become obsolete, requiring ever more rule revisions and rulemakings Given the

---

[79] Written Remarks of Chairman Deborah Platt Majoras, Teaming Up Against Identity Theft: A Summit on Solutions, Los Angeles, CA, Feb. 23, 2006, *available at* http://www.ftc.gov/speeches/majoras/060223californiaidtheft.pdf. *See also* 16 C.F.R. § 314.3 (establishing that safeguards to protect customer information must be "appropriate to your size, and complexity, the nature and scope of your activities, and the sensitivity of the customer information at issue").

[80] The GLBA Safeguards Rule-type requirements include establishing a written information security program that has "reasonable" physical, technical and procedural safeguards to ensure the security and confidentiality of PII. 16 C.F.R. § 310.3(a). The process begins with a risk assessment, which is unique to each organization and requires companies to evaluate the nature and risks of their particular information systems and the sensitivity of the information they maintain. 16 C.F.R. § 310.4(b). There are various examples of "physical, technical and procedural safeguards" but there are no explicit mandates. Companies' programs must be reasonable, and must be reviewed and revised on an ongoing basis to take into account evolving threats and technologies. 16 C.F.R. § 310.4(c) and (e).

number of disadvantages associated with implementing specific practices, if the Commission does find it necessary to act, it should require companies to adhere to a standard of reasonableness.

B. The Commission Should Not Mandate Consumer-Set Passwords.

The Commission is considering whether carriers should be required to adopt a "consumer-set password system" for consumers to access CPNI,[81] and has asked whether this rule would materially increase the security of CPNI.[82] While consumer-set password mandates might be part of a particular company's approach to securing CPNI, a rule requirement applicable to all companies goes too far. Consumer-set passwords are not consumer friendly, and would not materially increase security. Although passwords do provide an additional step in controlling access, ultimately, they can sometimes just be another tool for wrongdoers, that, once obtained, makes CPNI or other sensitive information readily available for unauthorized access. Accordingly, requiring consumer set passwords as a means to control access to CPNI will not materially increase the security of CPNI, and in some instances can make PII more vulnerable than not. In addition, because technology is constantly evolving, mandating consumer set passwords or any specific technology would be unwise, as it may quickly become outdated.

Surprisingly, consumer-set passwords are not consumer friendly. In fact, the majority of consumers would rather not use a unique password. In a recent study by the Ponemon Institute, nearly 60% of consumers responding to a poll would rather not provide a unique password plus a personal fact to a company for account access.[83] Moreover, 87% of poll respondents say that

---

[81] *CPNI NPRM* ¶¶ 15-16.

[82] *Id.* ¶ 16.

[83] Ponemon Report, Those Pesky Passwords, Larry Ponemon, CSO ONLINE.COM, March 2006, *available at* http://www.csoonline.com/read/030106/ponemon.html?action=print. (hereinafter *Ponemon Report*).

they are opposed to legislatively mandated password requirements[84] and only 12% said that new government regulations should require companies to use passwords to identify customers.[85]

In addition to not being consumer friendly, password protection mechanisms are generally ineffective at controlling access to information. This is primarily due to the pervasiveness of electronic access environments requiring a password.[86] As a result of having to remember so many passwords in numerous situations, most users have resorted to writing their password down on paper, sharing it, using the same one for all applications, and/or never changing it.[87] These practices jeopardize the security of passwords. Passwords can also be stolen or guessed,[88] and powerful password cracking tools can decrypt a password within minutes or hours.[89] In addition, consumers' use of the same password on multiple accounts is one of the most vulnerable aspects of any password-enabled system – once a person's password has been exposed, that person's entire digital identity may be vulnerable to disclosure.[90] For example, in April 2005, information broker LexisNexis reported that intruders had accessed PII

---

[84] *Id.* at Bar Chart 2.

[85] *Id.* at Table 6.

[86] *See* Universal Authenticated Logon, A White Paper, CRYPTOCARD CORP., at 1 (2003), *available at* http://www.opsec.com/solutions/partners/downloads/cryptocard-whitepaper.pdf (hereinafter *CryptoCard White Paper*).

[87] *Id.*

[88] *See* Jay Lyman, *More Keyloggers Swiping Identity Info*, ECOMMERCETIMES, Nov. 16, 2005, http://www.ecommercetimes.com/story/47399.html (reporting that keyloggers and other malicious software viruses and Trojan horses are increasing in sophistication and ability to record a user's password).

[89] *See Passwords: Why They Are So Easy to Crack*, SIGNIFY WHITE PAPER, at 1, *available at* http://www.signify.net/uploads/Passwords-why-they-are-so-easy-to-crack.pdf (hereinafter *Signify White Paper*).

[90] *See id.*

of as many as 280,000 individuals using the passwords of customers of its subsidiary, Seisint.[91] The company was not even aware of unauthorized access until it began integration activities in February 2005 after purchasing the Seisint business in July 2004. LexisNexis confirmed that neither its network nor Seisnet's network was hacked into or penetrated,[92] perhaps suggesting that the intruders obtained the passwords from a separate source, which if true, would illustrate the vulnerability of accounts after disclosure of consumers' passwords.

As with any technological mandate, password protections can be quickly surpassed by technological advancements. Locking in consumer set passwords by rule would leave carriers hamstrung if other technologies are developed that provide greater protection for consumers. As the Ponemon Report concluded, "[a]uthentication using passwords is viewed as inconvenient and perhaps outdated."[93] In fact, the Ponemon Report noted that, as an alternative, "[b]iometrics would seem to offer both the security and convenience companies and consumers are seeking,"[94] implying that passwords may already be technologically outdated.[95]

A business' decision to require that customers provide a password is not necessarily a bad practice, but the pitfalls should not be ignored. Consumers already have too many passwords to remember, many people use weak, static passwords, and passwords can be compromised.[96]

---

[91] Press Release, LexisNexis Begins Mailing Notifications Today to Individuals Whose Information May Have Been Fraudulently Accessed (April 18, 2005), *available at* http://www.lexisnexis.com/about/releases/0790.asp.

[92] *Id.*

[93] *Ponemon Report, supra* note 83.

[94] *Id.*

[95] *See also* Verisign to Form Security Network Driven by Devices, WALL STREET JOURNAL, Feb. 13, 2006 (reporting that Verisign "unveiled a common system that will allows multiple companies to provide secure access to online accounts with pocket-sized security devices, rather than relying on passwords alone").

[96] *See CryptoCard White Paper, supra* note 86, at 2.

Consequently, requiring carriers to implement a password protection mechanism will not materially enhance the security of CPNI. Instead, carriers should be free to develop security systems, which may or may not include passwords, that best fit their particular organization's requirements and customer needs.

C. The Commission Should Not Mandate Encryption of Stored Data.

The Commission is considering a mandate that CPNI data stored by a carrier must be encrypted, with the intent that encryption will better protect stored data from unauthorized disclosure.[97] But encryption of stored data primarily addresses efforts by hackers and other direct attacks on a company's system. Any rule requiring CPNI encryption would only add substantial cost to carriers without adding any additional protection from pretexting and other fraudulent activities by which the majority of CPNI is obtained. Charter itself utilizes a wide array of methods to maintain network security and is not aware of any instance where its CPNI has been compromised by hacking.[98] And as explained above, there is always a risk with specific technology mandates; at most, the Commission should impose reasonable protections on a case-by-case basis.

Encryption does not protect against pretexting and other fraudulent means of obtaining CPNI. If a data broker has the requisite customer personal information to deceive a customer service representative into believing that the data broker is the real customer, notwithstanding other company safeguards, no amount of encryption will prevent that representative from decrypting the CPNI and disclosing it to the "customer" under authorized procedures. Similarly, the unscrupulous employee with the authority to disclose CPNI necessarily has the authority to

---

[97] *CPNI NPRM* ¶ 19.

[98] As discussed at *supra*, note 19, Charter is not providing specifics on its practices.

decrypt CPNI and provide it to a third-party. Encryption technology, by itself, does not distinguish between authorized and unauthorized decryption and disclosure.[99]

Not only is encryption ineffective at preventing pretexting, it is also an expensive option for any company to undertake. Although the cost of the technology itself may be negligible, the cost to implement and maintain such a system, including the decryption of data for authorized uses, can be substantial,[100] and this cost does not include training and other administrative costs. Not surprisingly, then, a company's decision to encrypt its data, and the type of encryption technology to employ, is highly dependant on whether the benefits of encrypting data outweigh not only the financial expenditures, but the costs associated with decreases in performance and data access speed. As one security research director stated, "encrypting data slows performance, even with today's high-powered processors, so security executives should carefully weigh the need for strong encryption versus speed deterioration."[101]

In today's climate, data integrity is an important aspect of any business, and not just for the sake of protecting information or regulatory compliance. Businesses, including telecommunications carriers, have a strong market incentive in protecting their customer's

---

[99] As discussed, the data breaches at LexisNexis were not due to hacking and other direct attack on the company's system. In the event that such an attack occurs, current federal and state computer laws are adequate to prosecute such behavior and deter future instances of such attacks. For example, the *Computer Fraud and Abuse Act* prohibits any unauthorized computer access, by third-parties or employees who do not have authorization from the true subscriber. *See* 18 U.S.C § 1030(a)(2)(B) (criminalizing the act of "intentionally access[ing] a computer without authorization . . . and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication." A "protected computer" is defined as "a computer . . . which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(B).).

[100] Alison Diana, *Benchmarking Encryption Technology*, ECOMMERCETIMES, Aug. 12, 2003, http://www.ecommercetimes.com/story/31311.html.

[101] *Id.* (quoting Ray Wagner, research director for information security strategies at Gartner).

information.[102] Whether this incentive compels a company to encrypt its data requires a comprehensive cost-benefit analysis that balances the benefits of encryption against the cost to a company's bottom line and its level of customer service.[103] In light of the fact that CPNI encryption would not have prevented the recent wave of CPNI disclosures, the decision to encrypt CPNI should ultimately remain a business decision, and not a regulatory mandate.

D. Data Retention Requirements are Unnecessary.

The Commission seeks comment on whether to require carriers to delete non-essential CPNI records, or, alternatively, whether to "de-identify" such records.[104] There is no evidence that there is a need for such requirements. A pretexter that can access a customer's recent customer billing records that have not yet been de-identified has access to sensitive data that can be just as damaging as if that customer's two-year old billing records are accessed. In any event, protecting older CPNI data is simply a good business practice that does not require a regulatory mandate. Charter, for example, already has security procedures in place anytime CPNI is requested, whether the request was for recent or older information. Moreover, Charter destroys older billing records within a relatively short timeframe, keeping records only as long as necessary to resolve consumer billing disputes and as required under the terms of some interconnection agreements in furtherance of carrier-to-carrier billing issues.

---

[102] *See supra* Section III.B (recognizing that companies have a strong market incentive in protecting customer information).

[103] *See* David Sims, *Forrester Looks at CRM Best Practices, Part 1: Overview*, TMC NET, Dec. 22, 2005 (quoting William Band, CRM analyst for Forrester Research, from "Best Practices For CRM Deployment," that "customer service is a distinct competitive advantage, in which enterprises spent $3 billion worldwide on new customer service software licenses in 2005"), http://www.tmcnet.com/channels/customer-care/articles/180-forrester-looks-crm-best-practices-part-1-overview.htm.

[104] *CPNI NPRM* ¶ 20.

The "de-identifying" approach – where a customer's PII is separated from transactional billing records – would be particularly costly and time-consuming without any corresponding benefit. Deleting entire records merely requires a carrier to identify CPNI that is older than a preset date and then delete it. To de-identify a record, the carrier must implement a more complex program that first identifies which CPNI is older than some preset date (unless all CPNI must immediately be de-identified) and then isolates the "data that identify a particular caller from the general transaction records."[105] Presumably, identifiable data would include the customer's name, address, and account number, as well as the customer's phone number. This information, however, may not appear just once, but multiple times throughout the customer's record. Thus, identifying and removing or encrypting such data requires a complex algorithm for parsing the record and removing every instance where identifiable data appears. This complex solution would be prohibitively expensive to implement, and would burden the carrier's system by requiring it to monitor and edit CPNI records for each and every consumer on a daily basis. And if only applied to older records, modifying such records would have no effect on the availability of more recent CPNI, which appears to be most vulnerable to unauthorized disclosure, and is ultimately unnecessary given Charter's retention policies. Even more significant would be the costs and administrative complexity of re-identifying records as necessary to respond to consumer or government requests.

There is also an inherent tension between destruction of records on the one hand and access to records for lawful purposes on the other. Charter receives numerous requests from law enforcement for confidential information. For example, Charter receives an average of 275 requests each month from law enforcement for either PII or CPNI and that number is growing.

---

[105] *Id.*

In addition, archived records are helpful in resolving disputes as well as providing historical information to customers. While destruction of records clearly helps keep the total number of records kept by a carrier to a more manageable amount and exposes less information to wrongdoers, law enforcement often needs records to be kept for longer periods of time so they are available for law enforcement investigations.[106] The conflict between protecting consumer privacy and accommodating law enforcement requests places the carrier in a difficult position.

E. The Commission's Notice Proposals Are Too Far-Reaching.

The Commission is considering whether to require companies to notify customers when the security of their CPNI may have been breached[107] or in other instances as a matter of routine when there has been disclosure of CPNI, regardless of whether there is any indication that there was a breach.[108] The Commission is also contemplating advance notification before the release of CPNI (for authorization verification); the form the notification should take (e.g., via email, voicemail, on billing statement); whether precautionary verification or post-release notification should be a customer choice on an opt-in or opt-out basis; and whether there should be obligations to notify the Commission about CPNI disclosures in certain instances.[109] All of these impose unnecessary added costs on carriers without any meaningful consumer benefit.

1. Advance Notice/Verification

---

[106] *See ISP Snooping Gaining Support*, CNET NEWS.COM, Apr. 14, 2006 (describing how Bush Administration officials and some members of Congress support the concept of legislatively requiring ISPs to retain data about customers' online activities so that the data would be available for law enforcement investigations), http://news.com.com/2102-1028_3-6061187.html?tag=st.util.print. The rationale put forth in support of that proposal could apply equally to CPNI.

[107] *CPNI NPRM* ¶ 23.

[108] *Id.*

[109] *Id.* ¶ 22.

Because of the actual cost and burden of an advanced notice or verification requirement on carriers and customers, without any corresponding benefit, such a rule is not justified. First, advance notice/verification would be a major administrative burden. Customer Service Representatives would need additional training on when and how a carrier would have to notify customers and there would have to be a mechanism established to ensure advance notice in every applicable instance. Second, customers, particularly those who do not read bill inserts and customer notices, no matter how well written, would be needlessly alarmed by receipt of emails or calls or other notices advising that their CPNI is being released, no matter how legitimate the purpose, resulting in customer confusion as to what their carrier is doing. Moreover, if the advance notice is not coupled with the ability to prohibit actual disclosure of CPNI for purposes that do not require customer consent, the notification would to a large extent be pointless and only anger those customers who would be upset to learn of any disclosure of PII, no matter how lawful or legitimate. Finally, advance notification/verification conflicts with some legal restrictions applicable to carriers when they are complying with law enforcement requests. For example, the *Electronic Communications Privacy Act* prohibits carriers from notifying customers about a law enforcement request.[110] But even if law enforcement requests were carved-out of any advance notification requirement, this would only add an additional administrative complication.

2. Post-Release Notice

The Commission contemplates two types of post-release notice: (1) when the security of CPNI may have been breached, and (2) routine notification after the release of any CPNI, "including incidents where the carrier has no grounds to suspect that the request is not

[110] *See* 18 U.S.C. §§ 2703(a) and (c)(2)-(3) (ECPA); *see also* 18 U.S.C. § 2511(2)(a)(ii) (Wiretap Act).

legitimate."[111] The latter requirement is particularly burdensome, largely for reasons identified above for pre-release notice. It would be an immense administrative burden on carriers to, in every instance where CPNI has been disclosed, provide notice to the customer. Also, as explained above, if there is no reason to believe information has been compromised, it is particularly annoying and unnecessarily alarming to customers who receive such contacts.

Even the requirement of notice where CPNI may have been breached is unnecessary. Charter recognizes that in some instances, security breach notifications may be of value to customers.[112] However, security breach notifications can also do more harm than good. In the *CPNI NPRM*, the Commission noted that EPIC suggested that notification be required if security of CPNI "may have been breached."[113] Such a standard sets a threshold that is far too low for a security breach notification requirement because it creates a substantial risk of over-notification. It can result in customers being overwhelmed with carrier breach notification notices that are not indicative of an actual problem, and therefore would be counterproductive as customers, hardened to such notices, begin to simply ignore them. Alternatively, relatively indiscriminate disclosures may worry consumers into placing fraud alerts on their accounts or cause them to cancel service and switch providers.[114] Overnotification can also unduly penalize a company when no actual threat to a customers' privacy has occurred.[115] Moreover, carriers may have to

---

[111] *CPNI NPRM* ¶ 23.

[112] Jaikumar Vijayan, *Breach Notification Laws: When Should Companies Tell All*, COMPUTERWORLD, March 2, 2006, *available at* http://www.computerworld.com /printthis/2006/0,4814,109161,00.html. (reporting that there is "value in telling consumers about security breaches that pose a real risk of identity theft or fraud").

[113] *CPNI NPRM* ¶ 21.

[114] Vijayan, *Breach Notification Laws: When Should Companies Tell All, supra* note 112.

[115] *See supra* note 26 (discussing reduction of company's stock prices as a result of disclosure of confidential information).

bear huge administrative costs to deliver notice in each and every instance where CPNI "may" have been compromised.

To the extent the Commission ultimately does require breach notification to consumers, Charter recommends a risk threshold that properly balances consumers' interests in being aware of actual and real, and not hypothetical, threats to privacy, and business interests in avoiding unnecessary compliance costs and administrative burdens. Accordingly, Charter recommends the notification threshold to be set either at the level of when there is a "significant risk" that CPNI has been breached, a "clear risk of danger or harm to the consumer,"[116] or perhaps an approach proposed in one of the pending CPNI bills, such as when a carrier "becomes or is made aware" of CPNI disclosure to a pretexter.[117] These types of risk threshold notice afford businesses a reasonable obligation to provide notice, while still ensuring that customers are aware of all incidents of serious concern.

F. New Audit Trail Requirements Are Excessive.

The Commission's current rules already require an audit trail for disclosures of CPNI to third parties or for marketing purposes.[118] The Commission previously considered and rejected extending an audit trail requirement for disclosures of CPNI to account holders as too costly. In its 1998 *Second Report and Order*, the Commission established an electronic audit trail requirement for all disclosures and for incidents of access to customer accounts.[119] Following enactment of the rule, there was intense industry opposition to the requirement, largely revolving

---

[116] Vijayan, *Breach Notification Laws: When Should Companies Tell All*, *supra* note 112 (citing recommendation of Kirk Herath, chief privacy officer and associate general counsel at Nationwide Mutual Insurance Co.).

[117] *See* S. 2389. Only two other of the ten CPNI bills pending in Congress, H.R. 4943 and H.R. 4662, contain security breach notification provisions.

[118] 47 C.F.R. § 64.2009(c).

[119] *Second Report and Order*, 13 F.C.C.R. at 8,198-99, ¶ 199.

around the significant costs carriers would incur to implement such a requirement. Numerous carriers cited costs in the millions of dollars to implement the audit trail requirement, ranging from Sprint's estimate of $19.6 million to AT&T's estimate of $270 million.[120]

In its *1999 Reconsideration Order*, the Commission recognized these additional costs and scaled back the audit trail requirements to those of the current rules, concluding that "on balance, such a potentially costly and burdensome rule does not justify its benefit."[121] That rationale for not extending the audit trail requirement holds true today. There is no indication that the costs to implement such requirements have lessened. To the contrary, the costs have likely increased. Expanding the audit trail requirements would impose excessive costs on carriers which in turn would burden consumers. Such a requirement could be particularly burdensome on recent entrants such as Charter, with relatively small voice customer numbers. These large expenses could impede Charter's ability to roll-out its services.

VI. EXTENSION OF RULES TO VOIP AND VOIP BASED SERVICES.

Out of good business practice and respect for its customers' privacy, Charter has voluntarily established company policies and procedures that conform to the Commission's CPNI rules for its VoIP based services. For example, it has promulgated privacy and CPNI policies, delivers such information to customers biannually, and honors customer's CPNI choices as required under the current regime. However, unless the Commission ultimately deems VoIP and VoIP based service a "telecommunications service" (vs. an "information service"), the Commission is without statutory authority in Section 222 of the Act to extend its rules to VoIP providers. By its very terms, Section 222 applies to "telecommunications carriers" offering

---

[120] *Reconsideration Order*, 13 F.C.C.R. at 14,472, ¶ 124.

[121] *Id.* at 14,474-475, ¶ 127.

"telecommunications services".[122] The regulatory classification of VoIP as either a telecommunications service or an information service should be resolved in the Commission's pending IP-enabled services rulemaking[123] prior to any extension of CPNI rules to that service. Because of Charter's general belief that additional CPNI rules are unnecessary, it objects to extending the rules, particularly any rules that go beyond the current regime, to VoIP providers.

VII. ENFORCEMENT

As stated throughout these Comments, Charter strongly opposes the imposition of new CPNI rule requirements on telecommunications carriers. However, to the extent the Commission does enact new rules, Charter agrees with establishing a safe harbor under the rules for meeting certain minimum standards. Moreover, Charter is opposed to any rule where failure to meet minimum safe harbor requirements would automatically result in a violation of the rules without further inquiry.

VIII. CONCLUSION

For the reasons set forth above, the Commission should not adopt any of EPIC's proposals for new rules. EPIC's proposals would impose significant costs on carriers without any appreciable benefit to consumers. Consumers would actually be harmed because those costs would translate into higher bills and because of the resulting slowdown in the availability of alternative providers as companies like Charter would have investment dollars siphoned into complying with burdensome and unnecessary rules rather than launching service in new markets. Providers, particularly those such as Charter that are seeking to compete with established carriers and others new entrants in existing and new markets, already have incentives to protect CPNI.

---

[122] 47 U.S.C. § 222.

[123] *See* In the Matter of IP-Enabled Services, *Notice of Proposed Rulemaking*, 19 F.C.C.R. 4863 (2004).

Providers who do not adequately protect CPNI will lose customers or be unable to gain them. Accordingly, the best protection for CPNI is through vigorous pursuit of pretexters – the source of the problem – coupled with the Commission's current rules, which already impose significant obligations on telecommunications carriers.

Respectfully submitted,

CHARTER COMMUNICATIONS, INC.

By: /s/

John D. Seiver
Timothy P. Tobin
Brian J. Hurh
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
(202) 659-9750

Attorneys for Charter Communications, Inc.

Christin McMeley
Vice President & Senior Counsel
Privacy and Regulatory
Charter Communications, Inc.
12405 Powerscourt Drive
St. Louis, MO 63131

April 28, 2006